Secure Multiplex Coding with a Common Message

Ryutaroh Matsumoto
Department of Communications and Integrated Systems,
Tokyo Instiutte of Technology, 152-8550 Japan

Masahito Hayashi
Graduate School of Information Sciences,
Tohoku University, 980-8579 Japan
and Centre for Quantum Technologies,
National University of Singapore,
3 Science Drive 2, Singapore 117542

***Abstract*—We determine the capacity region of the secure multiplex coding with a common message, and evaluate the mutual information and the equivocation rate of a collection of secret messages to the second receiver (eavesdropper), which were not evaluated by Yamamoto et al.**

***Index Terms*—broadcast channel with confidential messages, information theoretic security, multiuser information theory**

I. Introduction

The information theoretic security attracts much attention recently [11], because it offers security that does not depend on a conjectured difficulty of some computational problem. One of most fundamental problems in the information theoretic security is coding for the wiretap channel considered by Wyner [14]. Later it was generalized to the broadcast channel with confidential messages (hereafter abbreviated as BCC) by Csiszár and Körner [4], in which there is a single sender called Alice and two receivers called Bob and Eve. In the formulation in [4], Alice has a common messages destined for both Bob and Eve and a private message destined solely for Bob. The word "confidential" means that Alice wants to prevent Eve from knowing much about the private message. The wiretap channel corresponds to BCC without the common message. The coding in these situations has two goals, namely error correction and secrecy.

The secrecy is realized by including random bits statistically independent of the secret message into the transmitted signal by Alice so that the secret message becomes ambiguous to Eve. The inclusion of random bits, of course, decreases the information rate. In order to get rid of the decrease in the information rate, Yamamoto et al. [8] proposed the secure multiplex coding, in which there is no loss of information rate. The idea of Yamamoto et al. is as follows. Suppose that Alice has T statistically independent messages $S_1, \ldots, S_T$. Then S_1, $\ldots$, S_{i-1}, S_{i+1}, $\ldots$, S_T serve as the random bits making S_i ambiguous to Eve, for each i. However, there are three rooms for improvement in Yamamoto et al. [8] as follows: (1) Let Z be Eve's received signal. Yamamoto et al. [8] proved that the mutual information $I(S_i; Z)$ can be made arbitrary small for each i, but they did not evaluate $I(S_\mathcal{I}; Z)$, where $S_\mathcal{I}$ denotes the collection of secret messages $(S_i : i \in \mathcal{I})$. (2) They did not evaluate the equivocation rate when the information rates of secret messages are large. (3) Their coding scheme [8] cannot support a common message to both Bob and Eve as done by Csiszár and Körner [4].

In this paper, we shall present a coding scheme for the secure multiplex coding that uses the privacy amplification technique and that can support a common message to both Bob and Eve. We evaluate the mutual information for collections of secret messages $(S_i : i \in \mathcal{I})$ for all $\emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T\}$. We also clarify the convergence speed of the mutual information to the infinity when the information rates of secret messages are large. The coding scheme in this paper is similar to the privacy amplification based scheme with the strong secrecy for BCC [12], but it differs in the following: Let F be a random variable of bijection from $S_1, \ldots, S_T$ to themselves. In order to apply the privacy amplification theorem to $S_1, \ldots$, S_T simultaneously, the correspondence between $F(S_1, \ldots, S_T)$ and S_i has to be the two-universal hashing [3] for each $i = 1$, $\ldots$, T. We shall also present how to construct such F.

This paper is organized as follows: Section II reviews relevant research results used in this paper. Section III introduces the strengthened version of the privacy amplification theorem, then defines and proves the capacity region of the secure multiplex coding with a common message, by using the strengthened privacy amplification theorem. Section IV presents constructions of the bijection F described in the previous paragraph. Section V concludes the paper.

II. Preliminary

A. Broadcast channels with confidential messages

Let Alice, Bob, and Eve be as defined in Section I. $\mathcal{X}$ denotes the channel input alphabet and $\mathcal{Y}$ (resp. $\mathcal{Z}$) denotes the channel output alphabet to Bob (resp. Eve). We assume that $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite unless otherwise stated. We shall discuss the continuous channel briefly in Remark 13. We denote the conditional probability of the channel to Bob (resp. Eve) by $P_{Y|X}$ (resp. $P_{Z|X}$). The set $\mathcal{S}_n$ denotes that of the private message and $\mathcal{E}_n$ does that of the common message when the block coding of length n is used. We shall define the achievability of a rate triple (R_1, R_e, R_0). For the notational convenience, we fix the base of logarithm, including one used in entropy and mutual information, to the base of natural logarithm. The privacy amplification theorem introduced in Theorem 5 is sensitive to choice of the base of logarithm.

Definition 1: The rate triple (R_1, R_e, R_0) is said to be *achievable* if there exists a sequence of Alice's stochastic encoder f_n from $\mathcal{S}_n \times \mathcal{E}_n$ to $\mathcal{X}^n$, Bob's deterministic decoder $\varphi_n : \mathcal{Y}^n \to \mathcal{S}_n \times \mathcal{E}_n$ and Eve's deterministic decoder $\psi_n : \mathcal{Z}^n \to$

$\mathcal{E}_n$ such that

$$\begin{aligned}
\lim_{n\to\infty} \Pr[(S_n, E_n) \neq \varphi_n(Y^n) \text{ or } E_n \neq \psi_n(Z^n)] &= 0,\\
\liminf_{n\to\infty} \frac{H(S_n|Z^n)}{n} &\geq R_e,\\
\liminf_{n\to\infty} \frac{\log|\mathcal{S}_n|}{n} &\geq R_1,\\
\liminf_{n\to\infty} \frac{\log|\mathcal{E}_n|}{n} &\geq R_0,
\end{aligned}$$

where S_n and E_n represents the secret and the common message, respectively, have the uniform distribution on $\mathcal{S}_n$ and $\mathcal{E}_n$, respectively, and Y^n and Z^n are the received signal by Bob and Eve, respectively, with the transmitted signal $f_n(S_n, E_n)$ and the channel transition probabilities $P_{Y|X}$, $P_{Z|X}$. The capacity region of the BCC is the closure of the achievable rate triples.

Theorem 2: [4] The capacity region for the BCC is given by the set of R_0, R_1 and R_e such that there exists a Markov chain $U \to V \to X \to YZ$ and

$$\begin{aligned}
R_1 + R_0 &\leq I(V;Y|U) + \min[I(U;Y), I(U;Z)],\\
R_0 &\leq \min[I(U;Y), I(U;Z)],\\
R_e &\leq I(V;Y|U) - I(V;Z|U),\\
R_e &\leq R_1.
\end{aligned}$$

As described in [11], U can be regarded as the common message, V the combination of the common and the private messages, and X the transmitted signal.

B. Broadcast channels with degraded message sets

If we set $R_e = 0$ in the BCC, the secrecy requirement is removed from BCC, and the coding problem is equivalent to the broadcast channel with degraded message sets (abbreviated as BCD) considered by Körner and Marton [9].

Corollary 3: The capacity region of the BCD is given by the set of R_0 and R_1' such that there exists a Markov chain $U \to V = X \to YZ$ and

$$\begin{aligned}
R_0 &\leq \min[I(U;Y), I(U;Z)],\\
R_0 + R_1' &\leq I(V;Y|U) + \min[I(U;Y), I(U;Z)].
\end{aligned}$$

One of several typical proofs for the direct part of BCD is as follows [2]: Given P_{UV}, R_0, R_1', we randomly choose $\exp(nR_0)$ codewords of length n according to P_U^n, and for each created codeword u^n, randomly choose $\exp(nR_1')$ codewords of length n according to $P_{V|U}^n(\cdot|u^n)$. Over the constructed ensemble of codebooks, we calculate the average decoding probability by the joint typical decoding, or the maximum likelihood decoding, etc.

C. Two-universal hash functions

We shall use a family of two-universal hash functions [3] for the privacy amplification theorem introduced later.

Definition 4: Let $\mathcal{F}$ be a set of functions from $\mathcal{S}_1$ to $\mathcal{S}_2$, and F the not necessarily uniform random variable on $\mathcal{F}$. If for any $x_1 \neq x_2 \in \mathcal{S}_1$ we have

$$\Pr[F(x_1) = F(x_2)] \leq \frac{1}{|\mathcal{S}_2|},$$

then $\mathcal{F}$ is said to be a *family of two-universal hash functions*.

III. Secure multiplex coding with a common message

A. Strengthened privacy amplification theorem

In order to analyze the equivocation rate, we need to strengthen the privacy amplification theorem originally appeared in [1], [6].

Theorem 5: (Extension of [6]) Let L be a random variable with a finite alphabet $\mathcal{L}$ and Z any random variable. Let $\mathcal{F}$ be a family of two-universal hash functions from $\mathcal{L}$ to $\mathcal{M}$, and F be a random variable on $\mathcal{F}$ statistically independent of L. Then

$$\mathbf{E}_f \exp(\rho I(F(L);Z|F=f)) \leq 1 + |\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho] \quad (1)$$

for $0 < \rho \leq 1$. If Z is not discrete RV, $I(F(L);Z|F)$ is defined to be $H(F(L)|F) - \mathbf{E}_z H(F(L)|F, Z=z)$.

In addition to the above assumptions, when L is uniformly distributed, we have

$$|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho] = \frac{|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho P_L(L)^{-\rho}]}{|\mathcal{L}|^\rho}. \quad (2)$$

In addition to all of the above assumptions, when Z is a discrete random variable, we have

$$\frac{|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho P_L(L)^{-\rho}]}{|\mathcal{L}|^\rho} = \frac{|\mathcal{M}|^\rho}{|\mathcal{L}|^\rho} \sum_{z,\ell} P_L(\ell) P_{Z|L}(z|\ell)^{1+\rho} P_Z(z)^{-\rho}. \quad (3)$$

Proof. See [13, Appendix]. ∎

Remark 6: It was assumed that Z was discrete in [13]. However, when the alphabet of L is finite, there is no difficulty to extend the original result.

As in [6] we introduce the following two functions.

Definition 7:

$$\begin{aligned}
\psi(\rho, P_{Z|L}, P_L) &= \log \sum_z \sum_\ell P_L(\ell) P_{Z|L}(z|\ell)^{1+\rho} P_Z(z)^{-\rho}, \quad (4)\\
\phi(\rho, P_{Z|L}, P_L) &= \log \sum_z \left(\sum_\ell P_L(\ell) (P_{Z|L}(z|\ell)^{1/(1-\rho)}) \right)^{1-\rho} \quad (5)
\end{aligned}$$

Observe that ϕ is essentially Gallager's function E_0 [5].

Proposition 8: [5], [6] $\exp(\phi(\rho, P_{Z|L}, P_L))$ is concave with respect to P_L with fixed $0 < \rho < 1$ and $P_{Z|L}$. For fixed $0 < \rho < 1$, P_L and $P_{Z|L}$ we have

$$\exp(\psi(\rho, P_{Z|L}, P_L)) \leq \exp(\phi(\rho, P_{Z|L}, P_L)). \quad (6)$$

B. Capacity region of the secure multiplex coding

Definition 9: The rate tuple (R_0, R_1, …, R_T) and the equivocation rate tuple $\{R_{e,\mathcal{I}} \mid \emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T\}\}$ are said to be *achievable* for the secure multiplex coding with T secret messages if there exists a sequence of Alice's stochastic encoder f_n from $\mathcal{S}_{1,n} \times \cdots \times \mathcal{S}_{T,n} \times \mathcal{E}_n$ to $\mathcal{X}^n$, Bob's deterministic decoder $\varphi_n : \mathcal{Y}^n \to \mathcal{S}_{1,n} \times \cdots \times \mathcal{S}_{T,n} \times \mathcal{E}_n$ and Eve's deterministic decoder $\psi_n : \mathcal{Z}^n \to \mathcal{E}_n$ such that

$$\begin{aligned}
\lim_{n\to\infty} \Pr[(S_{1,n}, \ldots, S_{T,n}, E_n) \neq \varphi_n(Y^n) \text{ or}\\
E_n \neq \psi_n(Z^n)] = 0,
\end{aligned}$$

$$\lim_{n\to\infty} I(S_{\mathcal{I},n}; Z^n) = 0\Big(\text{if } R_{e,\mathcal{I}} = \sum_{i\in\mathcal{I}} R_i\Big),$$
$$\liminf_{n\to\infty} H(S_{\mathcal{I},n}|Z^n)/n \geq R_{e,\mathcal{I}},$$
$$\liminf_{n\to\infty} \frac{\log|\mathcal{S}_{i,n}|}{n} \geq R_i,$$
$$\liminf_{n\to\infty} \frac{\log|\mathcal{E}_n|}{n} \geq R_0,$$

for $i = 1, \ldots, T$, where $S_{i,n}$ and E_n represent the i-th secret and the common message, respectively, $S_{i,n}$ and E_n have the uniform distribution on $\mathcal{S}_{i,n}$ and $\mathcal{E}_n$, respectively, $S_{\mathcal{I},n}$ is the collection of random variables $S_{i,n}$ with $i \in \mathcal{I}$, and Y^n and Z^n are the received signal by Bob and Eve, respectively, with the transmitted signal $f_n(S_{1,n}, \ldots, S_{T,n}, E_n)$ and the channel transition probabilities $P_{Y|X}$, $P_{Z|X}$. The capacity region of the secure multiplex coding is the closure of the achievable rate tuples.

Theorem 10: The capacity region for the secure multiplex coding with a common message is given by the set of R_0, R_1, $\ldots$, R_T and $\{R_{e,\mathcal{I}} \mid \emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T\}\}$ such that there exists a Markov chain $U \to V \to X \to YZ$ and

$$\begin{aligned}
R_0 &\leq \min[I(U;Y), I(U;Z)],\\
\sum_{i=0}^{T} R_i &\leq I(V;Y|U) + \min[I(U;Y), I(U;Z)]\\
R_{e,\mathcal{I}} &\leq I(V;Y|U) - I(V;Z|U) \text{ for all } \emptyset \neq \mathcal{I} \subseteq \{1,\ldots,T\},\\
R_{e,\mathcal{I}} &\leq \sum_{i\in\mathcal{I}} R_i.
\end{aligned}$$

Proof. The converse part of this coding theorem follows from that for Theorem 2. We have to show the direct part.

Let $\mathcal{S}_{i,n}$ be the message set of the i-th secret message, and $S_{\mathcal{I},n} = (S_{i,n} : i \in \mathcal{I})$. Let the RV B_n on $\mathcal{B}_n$ denote the private message to Bob *without secrecy requirement*, E_n on $\mathcal{E}_n$ the common message to both Bob and Eve. Without loss of generality we may assume that $\mathcal{B}_n = \prod_{i=1}^{T+1} \mathcal{S}_{i,n}$, where the set $\mathcal{S}_{T+1}$ is the alphabet of randomness used by the stochastic encoder, and n denotes the code length. $(S_{1,n}, \ldots, S_{T,n}, S_{T+1,n})$ is assumed to be uniformly distributed, which implies the statistical independence of $(S_{1,n}, \ldots, S_{T,n}, S_{T+1,n})$. In Section IV we shall prove the existence of a set $\mathcal{F}_n$ of bijective maps from $\mathcal{B}_n$ to itself such that if F_n is the uniform random variable on $\mathcal{F}_n$ then $\alpha_{\mathcal{I}} \circ F_n$ is a family of two-universal hash functions from $\mathcal{B}_n$ to $\mathcal{S}_{i,n}$ for all $\emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T\}$, where $\alpha_{\mathcal{I}}$ is the projection from $\mathcal{B}_n$ to $\prod_{i\in\mathcal{I}} \mathcal{S}_{i,n}$.

Let Λ be an RV indicating selection of codebook in the random ensemble constructed in the way reviewed in Section II-B, $U^n = \Lambda(E_n)$ on $\mathcal{U}^n$ and $V^n = \Lambda(B_n, E_n)$ on $\mathcal{V}^n$ codewords for the BCD taking the random selection Λ taking into account, and Z^n Eve's received signal.

The structure of the transmitter and the receiver is as follows: Fix a bijective function $f_n \in \mathcal{F}_n$ and Alice and Bob agree on the choice of f_n. Given T secret messages $s_{1,n}$, $\ldots$, $s_{T,n}$, choose $s_{T+1,n}$ uniformly randomly from $\mathcal{S}_{T+1}$, treat $b_n = f_n^{-1}(s_{1,n}, \ldots, s_{T,n}, s_{T+1,n})$ as the private message to Bob, encode b_n along with the common message e_n by an encoder for the BCD, and get a codeword v^n. Apply the artificial noise to v^n according to the conditional probability distribution $P^n_{X|V}$ and get the transmitted signal x^n. Bob decodes the received signal and get b_n, then apply f_n to b_n to get $(s_{1,n}, \ldots, s_{T,n})$. This construction requires Alice and Bob to agree on the choice of f_n. We shall show that there exists at least one f_n that meets the requirements of secure multiplex coding.

Define $B'_n = F_n^{-1}(S_{1,n}, \ldots, S_{T,n}, S_{T+1,n})$. We want to apply the privacy amplification theorem to $I(\alpha_{\mathcal{I}}(F_n(B'_n)); Z^n|F_n)$ for an arbitrary fixed $\emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T\}$. To use the theorem we must ensure independence of F_n and B'_n. Since the conditional distribution of B'_n is always uniform regardless of the realization of F_n, we can see that F_n and B'_n are independent. It also follows that B'_n is uniformly distributed over $\mathcal{B}_n$. Denote B'_n by B_n. The remaining task is to find an upper bound on $I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n, \Lambda)$. Since the decoding error probability of the above scheme is not greater than that of the code for BCD, we do not have to analyze the decoding error probability.

Firstly, we consider $\mathbf{E}_{f_n} \exp(\rho I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n = f_n, \Lambda = \lambda))$ with fixed selection λ of Λ. In the following analysis, we do not make any assumption on the probability distribution of E_n except that $S_{1,n}, \ldots, S_{T+1,n}, E_n, F_n$ and Λ are statistically independent.

By the almost same argument as [12] with use of Eq. (1), we can see

$$\begin{aligned}
&\mathbf{E}_{f_n} \exp(\rho I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n = f_n, \Lambda = \lambda))\\
&\leq \mathbf{E}_{f_n} \exp(\rho I(\alpha_{\mathcal{I}}((F_n(B_n)); Z^n, E_n|F_n = f_n, \Lambda = \lambda))\\
&\text{(Giving the common message } E_n \text{ does not increase } I \text{ much.)}\\
&= \mathbf{E}_{f_n} \exp(\rho \sum_e P_{E_n}(e) I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n = f_n, E_n = e, \Lambda = \lambda))\\
&\leq \mathbf{E}_{f_n} \sum_e P_{E_n}(e) \exp(\rho I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n = f_n, E_n = e, \Lambda = \lambda))\\
&\leq 1 + \sum_e P_{E_n}(e) \frac{\exp(n\rho R_{\mathcal{I}})}{\exp(n\rho R_p)} \sum_{b,z} P_{B_n}(b) P_{Z^n|B_n,E_n,\Lambda=\lambda}(z|b,e)^{1+\rho}\\
&\qquad P_{Z^n|E_n=e,\Lambda=\lambda}(z)^{-\rho} \text{ (by Eqs. (1–3))}\\
&= 1 + \sum_e P_{E_n}(e) \exp(n\rho(R_{\mathcal{I}} - R_p) + \psi(\rho, P_{Z^n|V^n}, P_{V^n|E_n=e,\Lambda=\lambda}))\\
&\text{(by [12] and Eq. (4)),}\\
&\leq 1 + \sum_e P_{E_n}(e) \exp(n\rho(R_{\mathcal{I}} - R_p) + \phi(\rho, P_{Z^n|V^n}, P_{V^n|E_n=e,\Lambda=\lambda}))\\
&\qquad \text{(by Eq. (6))}
\end{aligned}$$

where

$$R_{\mathcal{I}} = \frac{\sum_{i\in\mathcal{I}} \log|\mathcal{S}_{i,n}|}{n}, \tag{7}$$
$$R_p = \frac{\log|\mathcal{B}_n|}{n}. \tag{8}$$

We shall average the above upper bound over Λ. By the almost same argument as [12], we can see

$$\exp(\rho \mathbf{E}_{f_n,\lambda} \sum_e P_{E_n}(e) I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n|F_n = f_n, \Lambda = \lambda, E_n = e)) \tag{9}$$

$$\le \mathbf{E}_{f_n,\lambda} \exp(\rho \sum_e P_{E_n}(e) I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n | F_n = f_n, \Lambda = \lambda, E_n = e))$$

$$= 1 + \left[\exp(\rho(R_{\mathcal{I}} - R_p)) \left(\sum_{u\in\mathcal{U}} P_U(u) \exp(\phi(\rho, P_{Z|V}, P_{V|U=u})) \right) \right]^n . \quad (10)$$

Taking the logarithm of Eqs. (9) and (10) we can see

$$\begin{aligned} & I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n, E_n | F_n, \Lambda)) \\ &= I(\alpha_{\mathcal{I}}(F_n(B_n)); Z^n | F_n, \Lambda, E_n)) \\ &\le \frac{1}{\rho} \log\{1 + [\exp(\rho(R_{\mathcal{I}} - R_p)) \\ &\quad \left(\sum_{u\in\mathcal{U}} P_U(u) \exp(\phi(\rho, P_{Z|V}, P_{V|U=u})) \right)]^n\} \\ &\le \frac{1}{\rho} \left[\exp(\rho(R_{\mathcal{I}} - R_p)) \left(\sum_{u\in\mathcal{U}} P_U(u) \exp(\phi(\rho, P_{Z|V}, P_{V|U=u})) \right) \right]^n \end{aligned} \quad (11)$$

We shall consider the limit of the above upper bound. Taking the logarithm of the upper bound (11) we have

$$- \log \rho + n\rho \times \left[R_{\mathcal{I}} - R_p + \underbrace{\frac{1}{\rho} \log\Big(\sum_{u\in\mathcal{U}} P_U(u) \exp(\phi(\rho, P_{Z|V}, P_{V|U=u})) \Big)}_{(*)} \right].$$

We can see that (*) $\to I(V;Z|U)$ as $\rho \to 0$ by applying the l'Hôpital's rule to (*).

Set the size of $\mathcal{B}_n$ as

$$\frac{\log|\mathcal{B}_n|}{n} = R_p = I(V;Y|U) - \delta$$

with $\delta > 0$ such that

$$R_{\mathcal{I}} - R_{e,\mathcal{I}} > R_{\mathcal{I}} - R_p + I(V;Z|U) \quad (12)$$

for all $\emptyset \ne \mathcal{I} \subseteq \{1, \ldots, T\}$. Then by Eq. (11), we can see that there exists $\epsilon_n \to 0 (n \to \infty)$ such that

$$I(S_{\mathcal{I}}; Z^n | F_n, \Lambda) \le \epsilon_n \quad (13)$$

if $R_{\mathcal{I}} = R_{e,\mathcal{I}}$. On the other hand, when $R_{\mathcal{I}} > R_{e,\mathcal{I}}$, by Eq. (10), we have

$$\begin{aligned} & \mathbf{E}_{f_n,\lambda} \exp(\rho I(S_{\mathcal{I}}; Z^n | F_n = f_n, \Lambda = \lambda)) \\ \le \quad & 1 + \exp(n\rho(R_{\mathcal{I}} - R_p + I(V;Z|U) + \epsilon(\rho))), \end{aligned} \quad (14)$$

where $\epsilon(\rho) \to 0 (\rho \to 0)$. Let δ_n be the decoding error probability of the underling channel code for BCD. Then, by the almost same argument as [13], there exists at least one pair of (f_n, λ) such that

$$\begin{aligned} & I(S_{\mathcal{I}}; Z^n | F_n, \Lambda) < 2 \cdot 2^T \epsilon_n \text{ (if } R_{\mathcal{I}} = R_{e,\mathcal{I}}), \\ & \exp(\rho I(S_{\mathcal{I}}; Z^n | F_n = f_n, \Lambda = \lambda)) \le 2 \cdot 2^T [1 + \exp(n\rho(R_{\mathcal{I}} - R_p + \\ & \qquad I(V;Z|U) + \epsilon(\rho)))], \quad (15) \\ & \text{decoding error probability} \le 2 \cdot 2^T \delta_n. \end{aligned}$$

By Eq. (15) we can see

$$\frac{I(S_{\mathcal{I}}; Z^n | F_n = f_n, \Lambda = \lambda)}{n} \le \frac{1 + \log(2 \cdot 2^T)}{n\rho} + R_{\mathcal{I}} - R_p + I(V;Z|U) + \epsilon(\rho). \quad (16)$$

for $R_{\mathcal{I}} - R_p + I(V;Z|U) + \epsilon(\rho) \ge 0$, where we used $\log(1 + \exp(x)) \le 1 + x$ for $x \ge 0$. By Eqs. (12) and (16) we can see that the equivocation rate $H(S_{\mathcal{I}} | Z^n, F_n = f_n, \Lambda = \lambda)/n$ becomes larger than the required value $R_{e,\mathcal{I}}$ for sufficiently large n. This completes the analysis of the equivocation rates and the mutual information for all $\emptyset \ne \mathcal{I} \subseteq \{1, \ldots, T\}$. ∎

Remark 11: Our proof does not require the common message E_n to be decoded by Bob. Our technique can provide an upper bound on the mutual information of $S_{\mathcal{I}}$ to Eve even when E_n is a private message to Eve.

Remark 12: The (negative) exponential decreasing rate of the mutual information in our argument is

$$\rho(R_{\mathcal{I}} - R_p) + \log \left[\sum_{u,v,z} P_{UVZ}(u,v,z) P_{Z|V}(z|v)^\rho P_{Z|U}(z|u)^{-\rho} \right] \quad (17)$$

when $R_{e,\mathcal{I}} = R_{\mathcal{I}}$. Minimizing the above expression over $0 < \rho \le 1$, R_p and $U \to V \to X \to YZ$ such that $R_0 \le \min\{I(U;Y), I(U;Z)\}$ and $R_p \le I(V;Y|U)$ gives the smallest negative exponent. From the form of the mathematical expression, increase in R_p decreases the mutual information and increases the decoding error probability of the secret message to Bob. This suggests that the optimal mutual information and the optimal decoding error probability cannot be realized simultaneously. We note that the exponent (17) is the same as one given by Yamamoto et al. [8] when there is no common message.

Remark 13: We can easily carry over our proof to the case of the channel being Gaussian, because

- we can extend Eq. (3) to the Gaussian case just by replacing the probability mass functions $P_{Z|L}$ and P_Z by their probability density functions.
- the random codebook Λ obeys the multidimensional Gaussian distribution,
- the concavity of ϕ is retained when its second argument is conditional probability density,
- and the all mathematical manipulations in this section remains valid when U, V, Z, Λ are continuous and their probability mass functions are replaced with probability density functions, while B_n, E_n, F_n remain to be discrete RVs on finite alphabets.

IV. Random permutations whose projections give two-universal hash functions

Let $\mathcal{S}_1, \ldots, \mathcal{S}_{T+1}$ be finite sets and $\mathcal{B} = \prod_{i=1}^{T+1} \mathcal{S}_i$. In Section III, we needed a set $\mathcal{F}$ of bijective maps from $\mathcal{B}$ to itself such that the uniform random variable F on $\mathcal{F}$ gives two-universal hash functions from $\mathcal{B}$ to $\mathcal{S}_i$ by $\alpha_{\mathcal{I}} \circ F$, where $\alpha_{\mathcal{I}}$ is the projection from $\mathcal{B}$ to $\prod_{i\in\mathcal{I}} \mathcal{S}_i$. In this section we shall present two such sets with increasing order of implementation efficiency.

Proposition 14: Suppose that $\mathcal{F}$ is the set of all permutations on $\mathcal{B}$, then $\alpha_{\mathcal{I}} \circ F$ forms a family of two-universal hash functions for all $\emptyset \neq \mathcal{I} \subseteq \{1, \ldots, T+1\}$.

Proof. Let $x_1 \neq x_2 \in \mathcal{B}$. We have $|\mathcal{F}| = |\mathcal{B}|!$. On the other hand, the number of permutations F such that $\alpha_{\mathcal{I}}(F(x_1)) = \alpha_{\mathcal{I}}(F(x_2))$ is given by

$$|\mathcal{B}| \times (-1 + \prod_{i \notin \mathcal{I}} |\mathcal{S}_i|) \times (|\mathcal{B}| - 2)!,$$

because the number of choices of $F(x_1)$ is $|\mathcal{B}|$, the number of choices of $F(x_2)$ given the choice of $F(x_1)$ is $(-1 + \prod_{i \notin \mathcal{I}} |\mathcal{S}_i|)$, and the number of choices for values of rest of elements under F is $(|\mathcal{B}| - 2)!$. Therefore,

$$\Pr[\alpha_1(F(x_1)) = \alpha_1(F(x_2))] = \frac{-1 + \prod_{i \notin \mathcal{I}} |\mathcal{S}_i|}{|\mathcal{B}| - 1} \leq \frac{1}{\prod_{i \in \mathcal{I}} |\mathcal{S}_i|},$$

which completes the proof. ∎

The above construction can be used with any set $\mathcal{B}$, but implementation of random permutations is costly. When $\mathcal{S}_i$ is a linear space over a finite field $\mathbf{F}_q$, we have a more efficient implementation.

Lemma 15: Let $\mathcal{L}$ be a subgroup of the group of all bijective linear maps on $\mathcal{B}$. For $\vec{x} \in \mathcal{B}$, the orbit $O(\vec{x})$ of $\vec{x}$ under the action of $\mathcal{L}$ is defined by

$$O(\vec{x}) = \{L\vec{x} \mid L \in \mathcal{L}\}.$$

The family of functions $\{\alpha_{\mathcal{I}} \circ L \mid L \in \mathcal{L}\}$ is a family of two-universal hash functions if and only if

$$\frac{|O(\vec{v}) \cap (\{\vec{0}\} \times \prod_{i \notin \mathcal{I}} \mathcal{S}_i)|}{|O(\vec{v})|} \leq \frac{1}{\prod_{i \in \mathcal{I}} |\mathcal{S}_i|}$$

for all $\vec{v} \in \mathcal{B} \setminus \{\vec{0}\}$

Proof. We have

$$\begin{aligned}
& \frac{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in \{\vec{0}\} \times \prod_{i \notin \mathcal{I}} \mathcal{S}_i\}|}{|\mathcal{L}|} \\
= & \frac{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in (\{\vec{0}\} \times \prod_{i \notin \mathcal{I}} \mathcal{S}_i)\}) \setminus \{\vec{0}\}|}{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in O(\vec{x}_1 - \vec{x}_2)\}|} \\
= & \frac{|O(\vec{x}_1 - \vec{x}_2) \cap (\{\vec{0}\} \times \prod_{i \notin \mathcal{I}} \mathcal{S}_i)\})|}{|O(\vec{x}_1 - \vec{x}_2)|}.
\end{aligned}$$

Renaming $\vec{x}_1 - \vec{x}_2$ to $\vec{v}$ proves the lemma. ∎

Proposition 16: If $\mathcal{L}$ is the set of all bijective linear maps on $\mathcal{B}$, then $\{\alpha_{\mathcal{I}} \circ L \mid L \in \mathcal{L}\}$ is a family of two-universal hash functions.

Proof. For a nonzero $\vec{v} \in \mathcal{B}$, we have $O(\vec{v}) = \mathcal{B} \setminus \{\vec{0}\}$, which implies

$$\begin{aligned}
|O(\vec{v})| &= |\mathcal{B}| - 1, \\
|O(\vec{v}) \cap (\{\vec{0}\} \times \prod_{i \notin \mathcal{I}} \mathcal{S}_i)\})| &= \frac{|\mathcal{B}|}{|\prod_{i \in \mathcal{I}} \mathcal{S}_i|} - 1.
\end{aligned}$$

By Lemma 15 we can see that the proposition is true. ∎

V. Conclusion

We have presented a coding scheme for the secure multiplex coding proposed by Yamamoto et al. [8]. Our coding scheme has two features: (1) evaluation of the mutual information between Eve's received signal and a collection of multiple secret messages, including the convergence speed to the infinity when the information rates of secret messages are large, and (2) support for a common message to both Bob and Eve.

We note that we can make the proposed encoder and decoder universal by replacing the channel code with the constant composition code used by Körner and Sgarro [10] as done in [7].

Acknowledgment

The first author would like to thank Prof. Hirosuke Yamamoto to teach him the secure multiplex coding. A part of this research was done during the first author's stay at the Institute of Network Coding, the Chinese University of Hong Kong, and he greatly appreciates the hospitality by Prof. Raymond Yeung. This research was partially supported by the MEXT Grant-in-Aid for Young Scientists (A) No. 20686026 and (B) No. 22760267, and Grant-in-Aid for Scientific Research (A) No. 23246071. The Center for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[2] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Inform. Theory*, vol. 19, no. 2, pp. 197–207, Mar. 1973.

[3] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. System Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, 1968.

[6] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.

[7] M. Hayashi and R. Matsumoto, "Universally attainable error and information exponents for the broadcast channels with confidential messages," Apr. 2011, arXiv:1104.4285.

[8] D. Kobayashi, H. Yamamoto, and T. Ogawa, "How to attain the ordinary channel capacity securely in wiretap channels," in *Proc. 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Oct. 2005, pp. 13–18, arXiv:cs/0509047.

[9] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[10] J. Körner and A. Sgarro, "Universally attainable error exponents for broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. 26, no. 6, pp. 670–679, Nov. 1980.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Hanover, MA, USA: NOW Publishers, 2009.

[12] R. Matsumoto and M. Hayashi, "Strong security and separated code constructions for the broadcast channels with confidential messages," 2011, arXiv:1010.0743.

[13] ——, "Secure multiplex network coding," in *Proc. IEEE NetCod 2011*, Beijing, China, Jul. 2011, p. to appear, arXiv:1102.3002.

[14] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.